02/11/2015

Sécurisation d'un routeur Cisco

V1

Lecaudey Etienne

Tutoriel 1.1 : Sécurisation d'un routeur Cisco		
Lecaudey Etienne	Version 1.0	02/11/2015

SOMMAIRE :

Table des matières :

Table des matières

Tutoriel 1.1 : Sécurisation d'un routeur Cisco		
Lecaudey Etienne	Version 1.0	02/11/2015

Objectifs :

L'objectif de cette procédure est de sécuriser un routeur Cisco pour améliorer la sécurité d'un routeur.

Information sur les versions:

Routeur	Cisco0	1800

Désactivation des services in-utiles :

Des services sont lancés par défaut sur les routeurs, certains sont très utiles et d'autres au contraire peuvent même s'avérer dangereux.

Le fait de désactiver un service permet d'éviter que ce dernier soit piraté par l'intermédiaire d'une faille. En désactivant certains service, cela permet de consommer moins d'espace mémoire et moins de temps processeur et seront donc plus performant.

Pour commencer, nous allons désactiver les « small servers » tels que « echo » (ports TCP et UDP numéro7), discard (ports TCP et UDP numéro 9), changen (ports TCP et UDP, numéro 19)

Avec les commandes :

```
Router(config)#no service tcp-small-servers
Router(config)#no service udp-small-servers
```

Ensuite, nous désactivons le service Bootp :

```
Router(config)#no ip bootp server
```

Et le service finger :

```
Router(config)#no ip finger
```

On désactiver aussi le service http :

```
Router(config)#no ip http server
Router(config)#no ip http secure-server
```

On désactive aussi le service CDP (Cisco Discovery Protocol)

```
no cdp run
```

On désactive le service de configuration à distance (telnet&ssh)

```
Router(config)#line vty 0 4
Router(config-line)#transport input none
```

On désactive aussi la recherche DNS :

```
Router(config-line)#no ip domain-lookup
```

On désactive la commande ip classless (si nous n'avons pas de sous-réseaux) :

```
Router(config)#no ip classless
```

On désactive les requêtes TFTP :

```
Router(config)#no service config
```

On désactive les broadcasts dirigés :

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#no ip directed-broadcast
```

On désactive le routage des redirections ICMP :

```
Router(config-if)#no ip redirects
```

On désactive le routage par la source :

```
Router(config)#no ip source-route
```

On désactive IP Unreachable :

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#no ip unreac
Router(config-if)#no ip unreachables
```

Sécurisation par mots de passe :

Pour commencer, nous allons configurer un mot de passe :

- Pour l'accès au mode privilégié
- Pour l'accès à la ligne console
- Pour l'accès Telnet
- Pour l'accès SSH

Pour l'accès au mode privilégié :

```
Router(config)#enable secret sio2a
```

Pour l'accès à la ligne console :

```
Router(config)#line console 0
Router(config-line)#login
% Login disabled on line 0, until 'password' is set
Router(config-line)#password sio2a
Router(config-line)#
```

Pour l'accès Telnet :

```
Router(config)#line vty 0 4
Router(config-line)#password sio2a
```

Pour le SSH :

Il faut définir un compte utilisateur :

```
Router(config)#username etienne password lecaudey
```

Définir un hostname qui sera utilisé pour générer la clé de chiffrement :

```
Router(config)#hostname etienne
```

Ensuite, nous devons définir un nom de domaine pour générer la clé de chiffrement

```
etienne(config)#ip domain-name etienne.com
```

Puis on génére la clé de chiffrement :

```
etienne(config)#crypto key generate rsa general-keys modulus 1024
```

Sécurisation des mots de passe :

```
Router(config)#service password-encryption
```

Ajouter une bannière au login :

Pour ajouter une bannière au login de connexions, nous utilisons la commande :

```
etienne(config)#banner motd
% Incomplete command.

etienne(config)#banner motd char
Enter TEXT message.  End with the character 'c'.
attention, acces reserve au personnel
```

Sauvegarder la configuration :

Pour cela, nous avons désactiver le pare-feu windows :

Telecharger tftp64

Puis lancer la commande : copy running-conf ftpd

Puis mettre l'adresse ip du serveur tftp

Puis pour prendre l'ios

Show flash

Ensuite copy flash : tftp

Entrer le nom du fichier se terminant par .bin

Ensuite l'adresse ip du serveur tftp

Pour restaurer la configuration :

Copy tftp running-config

Adresse ip du serveur et le nom du fichier du router

Protection de l'équipement

```
service tcp-keepalives-in ! Préviens les sessions orphelines
no logging console ! Empêche de bloquer le port console par trop de log
service password-encryption ! Cache les mots de passes dans les fichiers de
configuration
scheduler max-task-time 5000 ! Protège des plantages ou bloquage de process

! En cas de crash: Envois d'un DUMP sur un serveur FTP:

ip ftp username USER-CISCO-SUR-FTP-SRV ! Déclaration du compte FTP
ip ftp password PASSWORD-CISCO-SUR-FTP-SRV ! Déclaration du mot de passe
FTP
exception protocol ftp ! Déclare l'envoie du dump par FTP
exception dump IP-ADDRESS-FTP-SRV ! Adresse IP du serveur FTP
```

Protection juridique

```
banner login #
Attention !
Acces reserve au personnel du service informatique de NOM-ENTREPRISE.
Toutes activites sur ce systeme sont enregistrees.
Toutes preuves d activites non autorisees seront traitees par les autorites
competentes.
Toute intrusion sur un systeme informatique est interdite par les articles
323-1 a 323-7 du Code penal.#
banner motd #
Attention !
Acces reserve au personnel du service informatique de NOM-ENTREPRISE.
Toutes activites sur ce systeme sont enregistrees.
Toutes preuves d activites non autorisees seront traitees par les autorites
competentes.
Toute intrusion sur un systeme informatique est interdite par les articles
```

323-1 a 323-7 du Code penal.#

Activation du SSH

Version 12.2T ou fonctionnalités DES obligatoire

```
hostname NOM-MACHINE ! Nom de l'équipement
ip domain name CLIENT.FR ! Déclaration du nom de domaine (obligatoire pour le SSH)
crypto key generate rsa ! Génère la clef RSA : UTILISER UN MODULUS DE 1024 bits minimum !
line vty 0 4
transport input ssh ! N'accepte que le SSH
exec-timeout 70 0 ! Empêche une session orpheline de bloquer une ligne
!
```

Gestion des droits d'accès

Gestion des accès au routeur, l'avantage de gérer des utilisateurs fait que chaque modification de configuration est identifiée

```
enable secret MOT-DE-PASSE-ENABLE ! Mot de passe de l'accès super utilisateur
!
username NOM-UTILISATEUR1 secret MOT-DE-PASSE-UTILISATEUR1 ! Déclaration des users avec mot de passe crypté (version 12.2T minimum)
username NOM-UTILISATEUR1 password MOT-DE-PASSE-UTILISATEUR1 ! Déclaration des users (pour les versions IOS inférieures à la 12.2T)

! Activation du modèle sécurisé AAA:
!
aaa new-model ! Activation de l'AAA
!
aaa authentication login default local ! Utilise le paramétrage de la ligne par défaut
aaa authentication login Console none ! Déclaration du profil AAA « Console » n'utilisant pas d'authentification
aaa authorization exec default local ! Déclaration des droits d'accès locaux (dans le cas la gestion des niveau d'accès par login)
line con 0
login authentication Console ! Utilise le profil AAA « Console »
```

Sécurisation des interfaces

```
! Définition de l'access-list appliqué à une interface donnant sur Internet
ip access-list standard Bad-Traffic-from-Internet
deny 192.168.0.0 0.0.255.255 ! Adresses Source en 192.168.X.X
deny 10.0.0.0 0.255.255.255 ! Adresses Source en 10.X.X.X
deny 172.16.0.0 0.15.255.255 ! Adresses Source en 127.16.X.X à 172.32.X.X
deny 127.0.0.0 0.255.255.255 ! Adresse Source « localhost »
permit any ! Autorise Le reste
!
interface INTERFACE-NAME
no ip proxy-arp ! Désactivation du proxy-arp
ip verify unicast reverse-path ! Active l'Anti-spoofing (« ip cef »
obligatoire)
!

! Sécurité spéciale à ajouter au niveau des interfaces publiques uniquement
(lien WAN, etc…):
!
no cdp enable ! Désactivation du CDP
no ip redirects ! Empêche les redirections ICMP
no ip unreachables ! Ne renvois de message d'erreur ICMP unreachables
no ip directed-broadcast ! Evite les broadcast dirigés (ex: 192.168.1.255)
ip access-group Bad-Traffic-from-Internet in
!
```